Presentation of Specification to TSG or WG

Presentation to:	**TSG SA Meeting #24**
Document for presentation:	**TR 23.898, "Access Class Barring and Overload Protection"**
Version	**1.0.0**
Presented for:	**Information**

Abstract of document:

TR 23.898 studies 3GPP system enhancements (such as CS or PS domain specific access control etc…) to cope with several network overload and failure situations.

There are three general approaches to solve the overload or failure situations identified in the WID.

1- Existing RAN access control mechanisms to solve e.g. cell level and RNC/BSC overload
2- New Domain specific access control to solve e.g. MSC or SGSN overload/failure
3- Appropriate reject causes and Wait timers to solve e.g. Packet Backbone NW or GGSN overload/failure

Item 1 does not require any development other than a few recommendations for application of existing mechanisms.

Item 2 DSAC architecturual aspects have been extensively documented in clauses 5 and no outstanding issues are remaining.

A UE based solution has been discussed and endorsed by CN1 and SA2 for resolving the Gs interface specific case and is documented in clause 5.4.

Item 3 is still awaiting contributions but will mainly involve a few case studies and no architectual changes are expected.

TR23.898 is then considered more than 50% complete and is presented for information to the SA Plenary.

Changes since last presentation to TSG SA:

Not applicable. This is the first presentation.

Outstanding Issues:

- Documentation for item 1
- Item 3 Case studies and corresponding solutions
- Study other Overload situations if any

Contentious Issues:

None identified.

3GPP TR 23.898 V1.0.0 (2004-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access Class Barring and Overload Protection; (Release 6)

Select keywords from list provided in specs database.

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

Domain specific access control is required for congestion by natural disasters and node failure. In addition to the functions, it is available to enhance functions associating with access control barring and overload protection.

1 Scope

The present document describes required functionalities for domain specific access control on UTRAN and possible backward compatible enhancements to the 3GPP system's R97 (GPRS), R99 (UMTS) and Rel 5 ("Iu-flex").to ensure CS and PS Domain independent management.

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications ".

[2] 3GPP TS 22.011: "Service accessibility"

[3] 3GPP TS 25.331: "Radio Resource Control (RRC) Protocol Specification"

[4] 3GPP TS 23.236: "Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes"

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions apply.

Domain Specific Access Control: Access control functionality for access barring in each domain (i.e. CS domain or PS domain).

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply. Additional applicable abbreviations can be found in TR 21.905 [1].

DSAC Domain Specific Access Control

DSACR Domain Specific Access Control Restriction

4 Congestion and Failure Situations

Congestion and failure situations which would need improvement or enhancement in the current specifications are described below.

4.1 Congestion Situation

4.1.1 MSC/VLR or SGSN Congestion Situation

When external disasters (e.g. earthquakes) affect an entire MSC area, CS call are likely to increase. In this situation, if MSC/VLR congestion happens then CS calls should be restricted.

However, applying the current access class barring mechanism will restrict both CS calls and PS sessions.

In order to utilise the available capacity in PS domain, access class barring should be applied to each domain separately. A suitable Domain Specific Access Control or DSAC mechanism should be provided to allow the network to:

- Restrict the amount of traffic on the CS services; and
- Control the amount of traffic towards the PS domain in order to prevent the propagation of CS domain congestion to the PS domain.

Likewise, whenever the SGSN gets congested, DSAC can be also applied in order to utilize the CS node capacity.

4.2 Failure Situation

4.2.1 MSC/VLR or SGSN Failure Situation

When VLR/MSC or SGSN fails, CS calls or PS sessions from UEs should be prohibited.

However, applying the current access class barring mechanism would restrict traffic to both CS and PS domains.

In order to utilise the available capacity in the domain functioning normally, access class barring should be applied to each domain separately. Domain Specific Access Control or DSAC allows the network to control the amount of requests to each domain and congestion or failure of a domain caused by the failure of the other domain can then be prevented.

5 Architectural Concept

5.1 General overview

Editor's Note: The purpose of this sub-clause is to describe the general overview.

5.2 Domain Specific Access Control architecture aspects

To control or restrict access from UEs to a specific domain, it is natural to extend the existing access control mechanism specified in TS22.011 and TS25.331. The current mechanism limits the access from UEs in idle mode to the network regardless of a domain if the access class of the UE is barred according to the system information. Therefore, a solution is to extend the system information so that access class baring list can be specified for each domain (see 5.2.1).

Introduction of domain specific access control restriction means that UEs in idle mode may establish RRC connection if its access is toward the domain not restricted. It is therefore necessary to specify access control for UEs in RRC connected state so that its access to the restricted domain can be limited (See 5.2.2).

The principles for access control of UEs in connected mode are derived from the discussion in 5.2.2:

1) Change in domain specific access class restriction (DSACR) status shall be informed to the UE in connected mode.

2) Existing UTRAN procedures such as paging is sufficient for notification of DSACR status change.

3) Existing signalling connections to the domain to be restricted can be safely left as is, and

4) Objectives are to limit accesses from UEs to the specific domain sufficiently. Completeness should not be required.

Note: Provision of similar DSACR mechanism for GSM/GPRS is for further study.

5.2.1 DSAC solutions for UEs in idle mode

Taking advantage of currently available procedures, the system information broadcast by RNC is extended so that access class barring list can be specified for each domain. The example is shown in the Figure 5.2.1 where the part highlighted in green is the extension. When received such system information, possible UE behaviour is:

UE that does not support the feature: Act as “Access Class Barred list” is “0x0011”

UE that supports the feature that is initiating/terminating PS session: Act as “Access Class Barred list” is “0x0011”

UE that supports the feature that is initiating/terminating CS call: Act as “Not Barred”

Access Class Barred list	0x0011
CN domain identity	PS
Access Class Barred list-2nd Domain	Default
CN domain identity-2nd Domain	CS

Figure 5.2.1: Domain Specific Access Control in System Information (SIB3)

5.2.2 DSAC solutions for UEs in connected mode

On establishment of RRC connection, the UE saves DSACR status in its memory if the status is broadcast in the system information as shown in 5.3.1. The information is used within the UE to decide if setting up a signalling connection to a domain is allowed. Existing UTRAN procedures for paging and indication of system information change is utilized to inform the UE of changes in DSACR status. When receiving such notification, UE will read the system information and update the DSACR status saved in the UE.

The Figure 5.2.2 depicts a sequence example.

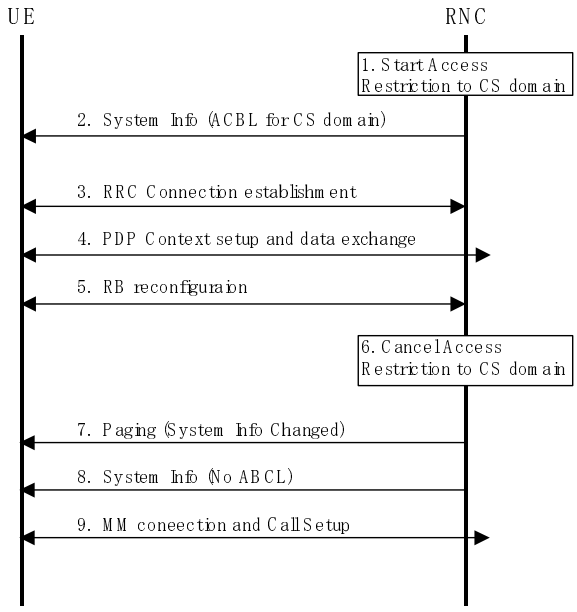

Figure 5.2.2: Example sequence for handling UEs in RRC connected state

1. The RNC detects MSC/VLR is overloaded, and it starts domain specific access control toward CS domain.
2. The RNC broadcasts DSACR information, i.e. access control barring list for CS domain in the system information.
3. The UE user starts web access application on his or her mobile and the UE establishes the RRC connection with the RNC to access PS domain, moving its status to RRC connected. The UE saves the DSACR information to CS domain in its memory.
4. The UE requests a PDP context and RB is setup for web access application. The request is transmitted to UTRAN since PS access is allowed according to the saved DSACR information.
5. The traffic on the RB is down to null and the RNC decides to put the UE in CELL_PCH state by UTRAN reconfiguration procedure.
6. The RNC detects that the MSC/VLR is not overloaded anymore and cancels domain specific access control toward CS domain by removing the DSACR information from the system information.
7. The RNC informs the UE of the change in DSACR information by the paging procedure to indicate system information change.

8. The UE reads the updated part of system information (no access control barring list for CS domain) and updates its DSACR status (no more access restriction to CS domain)

9. The UE user can now originate a CS call and the UE establishes the signalling connection to CS domain.

The solution does not cover the following cases. As discussed in the following subsections, the limitations do not cause severe problems. It can be concluded that special handling is not required.

1) UEs using dedicated channels

2) UEs with existing signalling connections to a domain to be restricted

3) UEs may be misinformed on availability of domain if the DRNC and SRNC are connected to different CN nodes

4) UEs missed Paging or System Information Change Indication will access the restricted domain

5.2.2.1 Handling of UEs with dedicated channels

Handling of UEs with dedicated channels is not necessary based on the analysis shown below.

1) Handling of UEs engaging in CS calls when CS domain becomes restricted.
   According to the year 2002 statistics published by Japanese Ministry of Public Management, Home Affairs, Posts and Telecommunications, the average duration of mobile originating CS calls is 122 seconds and CS calls less than 30 and 60 seconds account for 40% and 60% of all calls, respectively. Based on the statistics, if new call setup from idle mode UEs is prevented, it can be seen that congested situation would be mitigated quickly.

2) Handling of UEs using dedicated channels for PS services when PS domain becomes restricted
   Most of PS services provisioned have interactive nature. It is, therefore, expected that duration of staying dedicated mode is usually short. If there is not enough traffic, the RNC will switch the dedicated channels to common channels for the UE. Once the UE is put in the common channel state, then it can be notified of DSACR changes by the proposed method shown above. RNC may be able to prohibit the UE from going back to dedicated state to avoid increasing traffic to the congested the SGSN. It is also considered not likely the UE generates severe signalling load increase by requesting secondary PDP contexts or other PDP contexts.

3) Handling of UEs using dedicated channels for not restricted domain.
   The proportion of UEs using a dedicated channel over all UEs in MSC or SGSN area is, normally, considered to be low, particularly less than 5 %. Moreover the duration staying dedicated mode is considered as short based on the description 1) and 2) above. Therefore it is not likely that those UEs generate severe signalling load to the restricted domain.

5.2.2.2 Handling of existing signalling connections to a domain to be restricted

Handling such case is not necessary because:

1) Generating additional signalling load to the restricted domain using existing signalling connection such as requesting secondary PDP context is considered as infrequent.

2) The UE may generate user traffic using existing signalling connections. However, this is not as serious as signalling processing load in CN nodes, and

3) It is preferred to keeping impact to NAS as small as possible since introduction of DSAC functionality is wanted by operators as early as possible.

5.2.2.3 Handling of cases where DRNC and SRNC are connected to different CN nodes

There is a case where the UE may be misinformed on the availability of a domain when the DRNC and SRNC are connected to different CN nodes. For example, when the DRNC is connected to a congested node and the SRNC is connected to a CN node with normal condition, then the UE will be unnecessarily put under access restriction toward the domain. The issue can be solved by relocating UEs on boundary between RA and LA containing congested serving CN nodes.

It is for further study to check if SRNC relocation applied to UEs on the boundary of RA/LA may cause any problems to the congested CN node.

5.2.2.4 Handling UEs that missed DSACR information changes

If Paging or System Information Change Indication is not received, the UE may initiate Cell/URA update procedure or Initial Direct Transfer procedure for the access to the restricted domain. To handle such UE, the UTRAN procedures may be extended to indicate changes in system information. By setting appropriate repetition parameter in the procedures, however, probability of UEs missing the notification can be kept sufficiently low. We, therefore, propose that extension to the existing RRC procedures is not necessary. Moreover, impact to the existing implementation should be kept minimum since one of the primary application of DSAC is used in natural disasters. The sooner the availability is, the better.

Another possibility is for RNC to reject signalling connection request from the UE to the restricted domain. There is, however, no mechanism to prevent the UE to repeat the requests.

5.3 Access Control with Iu-flex

In a network configuration using Iu-flex, MSC/VLR or SGSN in the pool indicate overload situations to the RNC. The RNC routes initial NAS messages from UEs being served by an overloaded CN node to an available non-overloaded MSC/VLR or SGSN in the pool area. Consequently the UEs of the overloaded CN node(s) end up being served by non-overloaded MSC/VLRs or SGSNs in the pool area.

If multiple or all MSC/VLR or SGSN in the pool area indicate overload, the RNC may decide to use domain specific access control. This RNC decision is implementation specific.

Iu-flex does not require any other additional domain specific access control functionality on the Uu interface compared to network configurations without Iu-flex.

5.4 Domain Specific Access Control and Gs Interface

PS domain access restriction is applied as a result of the congestion and failure situations described in clause 4.

Under Network Operation Mode I, PS Domain Access Restriction prevents combined MM procedures to take place, which in turn may result in UEs becoming unreachable for mobile terminated CS services.

A solution should be provided to allow the UE to maintain its CS services despite the PS Domain restriction that is applied.

There are 2 possible solutions

1- A UE Based solution

2- A Network Operation mode change solution

5.4.1 UE based solution

This first solution introduces a new UE based procedure to maintain CS services when PS domain access class barring is applied.

This solution requires to introduce a new behaviour in the UE

The UE will react upon the received DSAC information (Access Class Barred List or ACBL) and will shift from Combined MM to Specific MM procedures, at the next periodic LA update or when the UE moves in another LA.

Figure 5.4.1.1 below shows the information flow for a UE receiving a DSAC information containing an ACBL corresponding to the start of a PS domain specific access control.

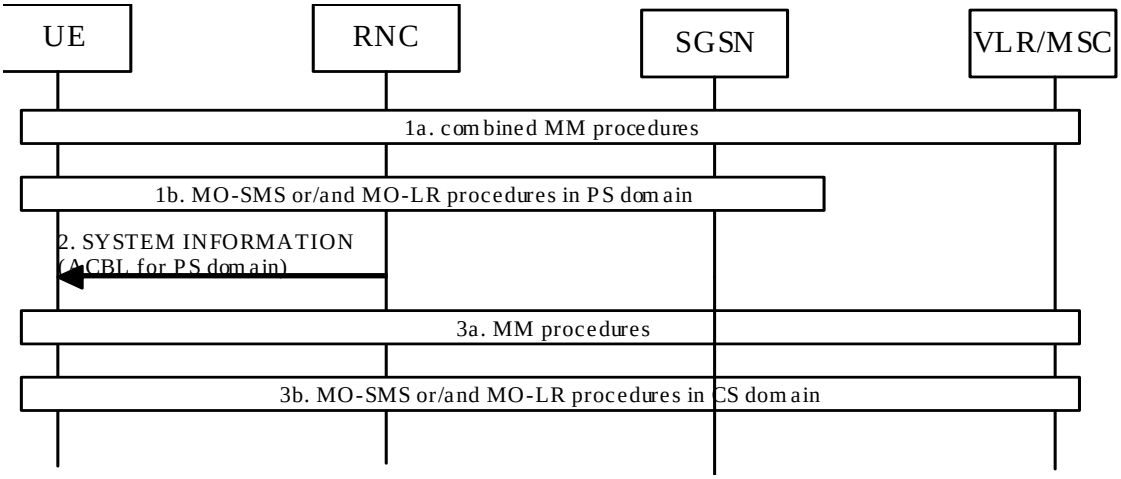

Figure 5.4.1.1: Start of a PS domain specific access control

Sequence description:

1. The network is in operation mode I before any congestion or failure

1a. UE performs combined MM procedures.

1b. The UE may perform MO-SMS and/or MO-LR procedures in PS domain.

2. The RNC detects SGSN overload or failure, then the RNC broadcasts system information with DSAC to the UE.

3. UE Behaviour during DSAC

3a. The UE stops performing combined MM procedures and starts performing specific MM procedure for CS domain, at the next periodic LA update or when the UE moves in another LA/RA.

3b. The UE immediately selects the CS domain if the UE needs to perform MO-SMS and/or MO-LR procedures.

Figure 5.4.1.2 below shows the information flow for a UE receiving a system information without any DSAC information corresponding to the end of PS domain specific access control

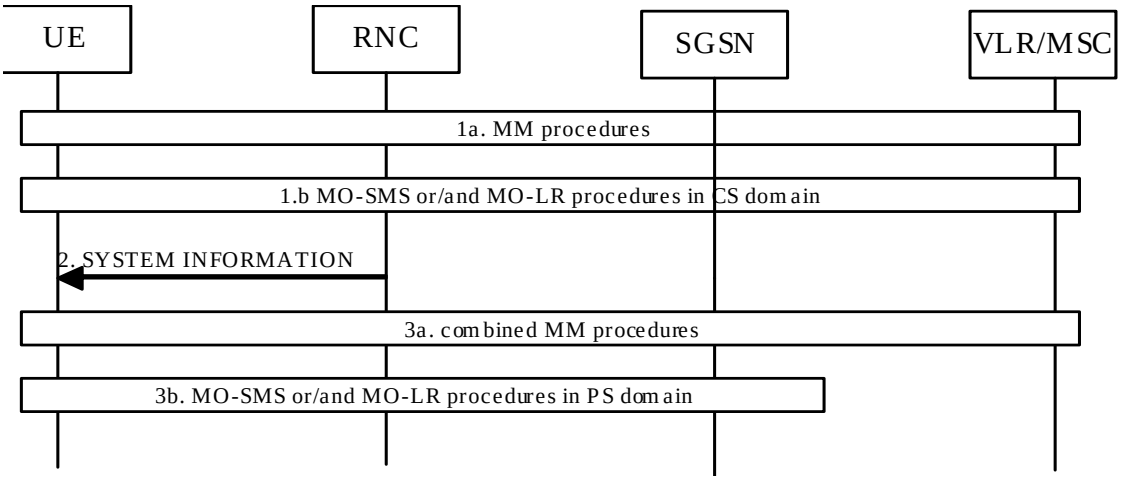

Figure 5.4.1.2: End of PS domain specific access control

Sequence description:

1. The UE is submitted to DSAC
1a. The UE performs CS domain specific MM procedures.

1b. The UE may perform CS domain MO-SMS and/or MO-LR procedures in the CS domain

2. The RNC detects that the SGSN has recovered, and it broadcasts system information without DSAC.

3. Network after recovery from congestion or failure
3a. The UE stops its specific MM procedures provisioning services and restarts Combined MM procedures, at the next periodic LA update or when the UE moves in another LA/RA.

3b. The UE resumes PS domain MO-SMS and/or MO-LR procedures

5.4.2 Network Operation Mode change (NMO change)

It should be noted that the UE behaviour at change of NMO is not explicitly specified in 3GPP specifications, but that most mobiles would perform location updates as soon as they detect a change of NMO from I to II.

When domain specific access control is applied, the 'NMO change' approach can seriously overload the serving CN node with many update procedures occurring at the same time, hence, it fails in its purpose with regards to overload protection.

5.4.3 Preferred Solution

The 'UE based' approach is preferred from the perspective of traffic handling and it should be chosen as the solution for Domain Specific Access Control with Gs Interface.

6 Conclusions

Annex A:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004.4	SA2#39	S2-041499			TR skeleton		0.0.0
2004.5	SA2#40	S2-041501			Domain Specific Access Control architecture aspects		
		S2-041605			Access Control with Iu-flex	0.0.0	0.1.0
		S2-042188			Vocabulary		
		S2-042202			Congestion and Failure Situations		
		S2-042203			Domain Specific Access Control and Gs Interface	0.1.0	0.2.0
2004.6	SA#24	SP-040332			Presented for information	0.2.0	1.0.0